BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

(11) **Japanese Unexamined Patent Publication No. HEI 09-214543**
(54) Title: Communication Path Control Methid and Communication Path Controller
(43) Date of Publication of Application: 15. 08. 1997
(19) Patent Office: JP
(21) Application No. 08-018917
(22) Date of Filing: 05.02.1996
(71) Applicant: Toshiba Corp.
(72) Inventors: INOUE Atsushi, ISHIYAMA Masahiro, MORIYA Osamu, SHINPO Atsushi, OKAMOTO Toshio
(51) Int. Cl : H04L 12/46, H04L 12/28, G06F 13/00, H04L 12/66

[Claims]

[Claim 1] A communication route control method in a computer network system connected to another computer network via a communication network, the computer network system being equipped with a home router unit which manages the current location of a computer whose home is at a predetermined location of connection in the private system network and relays a packet transmitted to a destination computer, the communication route control method for controlling a communication route between computers, the communication route control method comprising the steps of:

storing address information including a correspondence between a first location identifier which is unique to the computer and clearly defined in the private system network and a second location identifier which is clearly defined in the whole network so as to allow the location of a computer moving from the home position of connection among the computers to be identified;

judging, based on transmitting source information and destination information including a first location identifier included in a packet to be relayed by the home router unit, whether each of the computers communicating the packet with each other has moved from the home place of connection in the system network of its own or not; and

transmitting the second location identifier of the computer moving at least to a communicating partner of the computer moving in a case where it is judged that at least one of the two computers comminuting the packet with each other has moved from the home position of connection in the system network of its own.

--(omission)--

[0012]

[Means for Solving the Problems] The present invention (Claim 1) is directed to a communication route control method in a communication network system which is connected to another computer network via a communication network. The communication network system is equipped with a home router unit which manages the current location of a computer whose home is at a predetermined location of connection in the private system network and relays a packet transmitted to a destination computer. The communication route control method controls a communication route between computers. The communication route control method is characterized by storing address information including a correspondence between a first location identifier and a second location identifier. The first location identifier is unique to the computer and clearly defined in the private system network and a second location identifier which is clearly defined in the whole network so as to allow the location of a computer moving from the home position of connection among the computers to be identified. The communication route control method is also characterized by judging, based on transmitting source information and destination information including a first location identifier included in a packet to be relayed by the home router unit, whether each of the computers communicating the packet with each other has moved from the home place of connection in the system network of its own or not. Also, the communication route control method is characterized by transmitting the second location identifier of the computer moving at least to a communicating partner of the computer moving in a case where it is judged that at least one of the two computers comminuting the packet with each other has moved from the home position of connection in the system network of its own.

--(omission)--

[Embodiments of the Invention]

--(omission)--

[0034] First, with this embodiment, a description will be given in the case where moving host computers H2 and H3 are moving to private system networks 1b and 1c, respectively. When the host computer H2 and the host computer H3 as the communication partner communicate with each other through encryption, both host computers, as each other's current location is unconfirmed, each encipher and encapsulate a data packet including a destination being specified wtih a home address HA2 or HA3 allowing it to reach the home router HR (by using an address CA0, in the case of Fig. 4, which is clearly defined about the home router HR in the whole network), and send it out towards the home router HR of a private system network 1a to which the both host computers were connected before moving (① in Fig. 4).

[0035] Upon arrival of the data from the host computer H2, the home router HR decodes the enciphered data to know by the home address HA3 written in the header that the packet is addressed to the moving host computer H3. Then, the home router HR obtains the current location information of the moving host computer H3 with referring to such an address management table as that of Fig. 2 which is managed within the home router HR. In this case, since the destination address CA 3 of the move becomes the current location information, the destination is changed to the address CA 3 which is clearly defined in the whole network indicating the present location of the host computer H3, and then a data packet is sent to the host computer H3 (② in Fig. 4).

[0036] The same is applied to a communication carried out from the host computer H3 to the host computer H2. Specifically, the data (③ in Fig. 4) once sent out to the home router HR is decoded. Then, a data packet is sent to the host computer H2 after the destination is changed to the address CA2 whichis clearly defined in the whole network indicating the current location of the host computer H2 based on the current location information of the host computer H2 (④ in Fig. 4).

--(omission)--

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-214543
(43)Date of publication of application : 15.08.1997

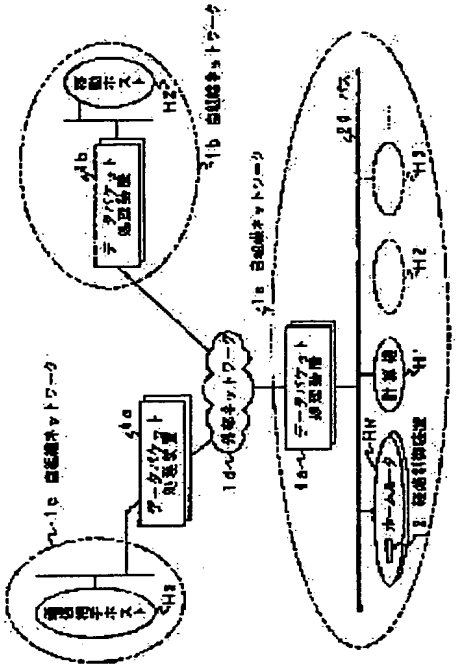
(51)Int.CI. H04L 12/46
H04L 12/28
G06F 13/00
H04L 12/66

(21)Application number : 08-018917
(22)Date of filing : 05.02.1996

(71)Applicant : TOSHIBA CORP
(72)Inventor : INOUE ATSUSHI
ISHIYAMA MASAHIRO
MORIYA OSAMU
SHINPO ATSUSHI
OKAMOTO TOSHIO

(54) COMMUNICATION PATH CONTROL METHOD AND COMMUNICATION PATH CONTROLLER

(57)Abstract:
PROBLEM TO BE SOLVED: To avoid redundancy communication at ciphering communication by detecting position information of a mobile computer and its communication opposite party and reporting each external network address with each other.
SOLUTION: Mobile host computers H2, H3 using self-organization network 1a as a home move respectively to external self-organization networks 1b, 1c. A path controller 12 references an address management table based on a transmission source address and a destination address in data packets via a home router HR to check whether or not both the computers are moving. In the case of detecting ciphering communication of a computer, a unique address as a whole in the network representing a current position of a communication opposite party is reported to the computers H2, H3. Thus, the position information of the mobile computer and the communication opposite party is detected and each external network address is reported to the both and control information representing direct connection is returned to the both not via a home router.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

実施例5

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－214543

(43)公開日　平成９年(1997)８月15日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ	12/46			Ｈ０４Ｌ	11/00	３１０Ｃ
	12/28			Ｇ０６Ｆ	13/00	３５５
Ｇ０６Ｆ	13/00	３５５	9466－5K	Ｈ０４Ｌ	11/20	Ｂ
Ｈ０４Ｌ	12/66					

審査請求　未請求　請求項の数６　ＯＬ　（全 14 頁）

(21)出願番号　特願平8－18917

(22)出願日　平成８年(1996)２月５日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　井上　淳
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

(72)発明者　石山　政浩
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

(72)発明者　森谷　修
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

(74)代理人　弁理士　鈴江　武彦

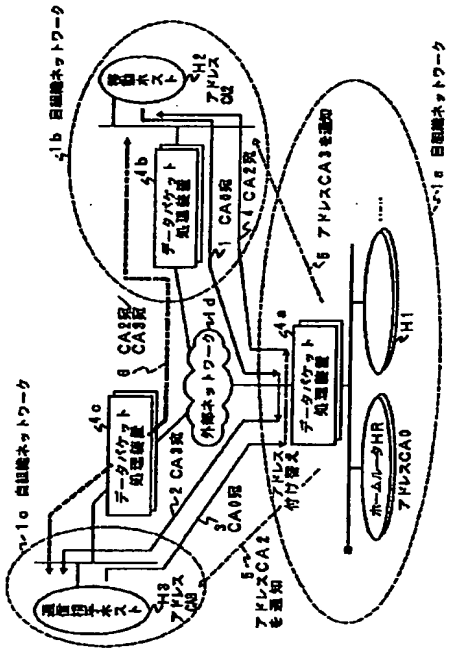
最終頁に続く

(54)【発明の名称】　通信経路制御方法および通信経路制御装置

(57)【要約】

【課題】　ホームルータを介して通信が行われる計算機ネットワークシステムにおいて、通信経路の冗長を回避可能な通信経路制御方法を提供すること。

【解決手段】　自組織ネットワーク内の所定接続位置をホームとする計算機の現在位置を管理し転送パケットを宛先計算機に中継するホームルータを持つシステムにて計算機間通信経路を制御する方法であって、計算機に固有の自組織ネットワーク内で一意の第１の位置識別子と移動中計算機の移動位置を識別可能なネットワーク全体で一意の第２の位置識別子の対応を記憶し、ホームルータで中継されるパケット内の送信元と宛先のアドレスと前記対応から該パケットを通信する計算機のうち少なくとも一方が自組織ネットワーク内のホームの接続位置から移動しているものであると判断された場合、少なくとも該移動している計算機の通信相手に該移動している計算機に対する前記第２の位置識別子を送信する。



1

【特許請求の範囲】

【請求項１】通信網を介して他の計算機ネットワークに接続され、自組織ネットワーク内の所定の接続位置をホームとする計算機の現在位置を管理し転送されてきたパケットを宛先計算機に中継するホームルータ装置を備えた計算機ネットワークシステムにおいて、計算機間の通信経路を制御するための通信経路制御方法であって、

前記計算機に固有の前記自組織ネットワーク内で一意に定められた第１の位置識別子と、該計算機のうちホームの接続位置から移動した計算機について該計算機が移動した位置を識別可能なネットワーク全体で一意に定められた第２の位置識別子とを対応付けたアドレス情報を記憶し、

前記ホームルータ装置により中継されるパケット内に含まれる前記第１の位置識別子からなる送信元情報および宛先情報と前記アドレス情報とに基づいて、前記パケットを通信する２つの計算機夫々について、前記自組織ネットワーク内のホームの接続位置から移動しているものであるか否かを判断し、

前記パケットを通信する２つの計算機のうち少なくとも一方が前記自組織ネットワーク内のホームの接続位置から移動しているものであると判断された場合、少なくとも該移動している計算機の通信相手に該移動している計算機に対する前記第２の位置識別子を送信することを特徴とする通信経路制御方法。

【請求項２】前記第２の位置識別子を送信した後に、前記自組織ネットワーク内の前記ホームルータ装置を前記２つの計算機間にて通信されるパケットが再度通過したことが検出された場合、前記第２の位置識別子の送信先の計算機に前記自組織ネットワーク内の前記ホームルータ装置を経由した通信を行なう旨の制御情報を送信することを特徴とする請求項１に記載の通信経路制御方法。

【請求項３】前記判断にあたって、前記送信元情報に対応する前記第２の位置識別子と前記宛先情報に対応する前記第２の位置識別子とを比較して、前記２つの計算機夫々が同一のネットワーク内に存在するか否かを判定し、

前記２つの計算機夫々が同一のネットワーク内に存在すると判定された場合、通信データに対するデータ加工処理を行わず最短の経路で直接通信するよう通信経路を変更することを指示する制御情報をも送信することを特徴とする請求項１に記載の通信経路制御方法。

【請求項４】前記判定にあたって、前記２つの計算機間で通信される通信データに対するデータ加工処理の内容が変更されるか否かをも併せて判定し、直接通信を確立させると変更が生じる場合、前記第２の位置識別子及び前記制御情報を双方に返信しないことを特徴とする請求項３に記載の通信経路制御方法。

【請求項５】前記判断にあたって、前記２つの計算機間で通信される通信データに対するデータ加工処理の内容

2

が変更されるか否かをも併せて判定し、直接通信を確立させると変更が生じる場合、前記制御情報に通信データのデータ加工処理の内容を変更させる指示情報を含めることを特徴とする請求項３に記載の通信経路制御方法。

【請求項６】通信網を介して他の計算機ネットワークに接続され、自組織ネットワーク内の所定の接続位置をホームとする計算機の現在位置を管理し転送されてきたパケットを宛先計算機に中継するホームルータ装置を備えた計算機ネットワークシステムにおいて、該自組織ネットワーク内の所定の接続位置をホームとする計算機間の通信経路を制御するための通信経路制御装置であって、

前記計算機に固有の前記自組織ネットワーク内で一意に定められた第１の位置識別子と、該計算機のうちホームの接続位置から移動した計算機について該計算機が移動した位置を識別可能なネットワーク全体で一意に定められた第２の位置識別子とを対応付けたアドレス情報を記憶する手段と、

前記ホームルータ装置により中継されるパケット内に含まれる前記第１の位置識別子からなる送信元情報および宛先情報と前記アドレス情報とに基づいて、前記パケットを通信する２つの計算機夫々について、前記自組織ネットワーク内のホームの接続位置から移動しているものであるか否かを判断する手段と、

前記パケットを通信する２つの計算機のうち少なくとも一方が前記自組織ネットワーク内のホームの接続位置から移動しているものであると判断された場合、少なくとも該移動している計算機の通信相手に該移動している計算機に対する前記第２の位置識別子を送信する手段とを備えたことを特徴とする通信経路制御装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、相互接続している複数のネットワーク間で相互にデータを交換する複数の計算機により構成される計算機システムにおいて、それらの計算機間の通信経路を制御する通信経路制御方法および通信経路制御装置に関する。

【０００２】

【従来の技術】計算機システムの小型化、低価格化やネットワーク環境の充実に伴って、計算機システムの利用は急速にかつ種々の分野に広く拡大し、また集中型システムから分散型システムへの移行が進んでいる。特に近年では計算機システム自体の進歩、能力向上に加え、コンピュータ・ネットワーク技術の発達・普及により、オフィス内のファイルやプリンタなどの資源共有のみならず、オフィス外あるいは一組織外とのコミュニケーション（例えば電子メール、電子ニュース、ファイルの転送など）が可能になり、これらが広く利用されはじめた。特に近年では、世界最大のコンピュータネットワーク「インターネット（Ｉｎｔｅｒｎｅｔ）」の利用が普及しており、インターネットと接続し、公開された情報、

サービスを利用したり、逆にインターネットを通してアクセスしてくる外部ユーザに対し、情報、サービスを提供することで、新たなコンピュータビジネスが開拓されている。また、インターネット利用に関して、新たな技術開発、展開がなされている。

【０００３】また、このようなネットワークの普及に伴い、移動通信（ｍｏｂｉｌｅ　ｃｏｍｐｕｔｉｎｇ）に対する技術開発も行われている。移動通信では、携帯型の端末、計算機を持ったユーザがネットワーク上を移動して通信する。ときには通信を行ないながらネットワーク上の位置を変えていくこともある。そのような通信において変化する移動計算機のネットワーク上のアドレスを管理し、正しく通信内容を到達させるために、ＩＥＴＦ／Ｍｏｂｉｌｅ－ＩＰ（参考文献：Ｃ．Ｐｅｒｋｉｎｇ（ＩＢＭ）：“ＩＰ　Ｍｏｂｉｌｅ　Ｓｕｐｐｏｒｔ（ｄｒａｆｔ－ｉｅｔｆ－ｍｏｂｉｌｅｉｐ－ｐｒｏｔｏｃｏｌ－１２．ｔｘｔ）”，Ｉｎｔｅｒｎｅｔ　Ｄｒａｆｔ，１９９５／８．）やＶＩＰ（参考文献：ＴａｒａｏｋａＦ．ｅｔ　ａｌ．“ＶＩＰ：Ａ　Ｐｒｏｔｏｃｏｌ　Ｐｒｏｖｉｄｉｎｇ　Ｈｏｓｔ　Ｍｏｂｉｌｉｔｙ，ＣＡＣＭ　Ｖｏｌ．３７，Ｎｏ．８（Ａｇｕ．１９９４）”）などの移動通信プロトコルが提案されている。

【０００４】また、ネットワークが普及し、ネットワーク間の自由な接続が実現され、膨大なデータ、サービスのやりとりがなされる場合、セキュリティ上の問題を考慮する必要が生じてくる。例えば、組織内部の秘密情報の外部ネットワークへの漏洩をいかに防ぐか、という問題や、組織外からの不正な侵入から、組織内ネットワークに接続された資源、情報をいかに守るか、という問題である。インターネットは、当初学術研究を目的に構築されたため、ネットワークの接続による自由なデータサービスのやりとりを重視しており、このようなセキュリティ上の問題は考慮されていなかったが、近年多くの企業、団体がインターネットに接続するようになり、セキュリティ上の問題から自組織ネットワークを防衛する機構が必要となってきた。

【０００５】そこで、複数のネットワークを接続する際に、それらのネットワークを介して相互にやりとりされるデータを監視、チェックし、不正なアクセスが外部から侵入したり、内部データが外部に漏洩することを防止する機構を配置することが一般に行われている。このような機構をファイアウォールという。ファイアウォールを設置することにより、外部への秘密情報の漏洩、外部からの不正なアクセスを防ぎ、かつ内部から安全に外部のサービスを受けられるようになる。

【０００６】また、特に機密性の高い重要データを外部ネットワークを介して通信する場合、外部にデータパケットを送出する前にその内容を暗号化し（必要に応じて認証コードを付加し）、受信したサイトで（認証コードを確認し）復号化する、という方法がある。この方法によれば、たとえ組織外のユーザが外部ネットワーク上のデータパケットを取り出しても、内容が暗号化されているので、決してその内容を漏洩することがなく、より安全な通信が確保できる。

【０００７】このような暗号化通信をサポートするファイアウォールで守られた（ガードされた）ネットワーク同士であれば相互に暗号化通信が可能であるが、前述の移動計算機へのアクセスを考えると、その計算機が移動前に属していたネットワークと同じ組織に管理されるネットワーク内に移動し、かつその移動先ネットワークがファイアウォールにガードされているなら、あたかも同じネットワーク内の計算機同士で通信するように暗号化通信ができる。一方、移動計算機が外部組織のネットワーク、または自組織のネットワークであってもファイアウォールされていないネットワークに移動した場合、その移動計算機は、外部の計算機として扱われなければならず、暗号化通信はできない。

【０００８】ところで、一般に移動通信を行う場合、移動計算機の移動先データを管理するホスト（例えばホームルータ）を置き、移動計算機への通信はそのホームルータを経由して行うことで移動計算機に対するデータの通信を行う。一般の通信の場合は、ホームルータ経由でよいが、もし移動計算機とその通信相手がいずれも同じ組織に管理されるネットワーク内にあり、かつファイアウォールでガードされている場合は、ホームルータを介することで冗長な通信を行ってしまう可能性がある。これは通信の開始時点では、移動計算機がどこのネットワークに移動しているかが未確定であるためである。

【０００９】

【発明が解決しようとする課題】従来は、移動通信においては、移動計算機の移動先データを管理するホームルータを置き、移動計算機への通信はそのホームルータを経由して行っていた。この場合、もし移動計算機とその通信相手がいずれも同じ組織に管理されるネットワーク内にあり、かつファイアウォールでガードされていて、相互に暗号化通信を行う場合、通信の開始時点では、移動計算機がどこのネットワークに移動しているかが未確定であるため、ホームルータを介した冗長な通信を行ってしまうことがある。この場合、両者が相互の外部ネットワークアドレス（すべてのネットワーク上で一意に定まっているアドレス）を知っていればホームルータを経由することなく暗号化通信が可能であり、通信効率も高い。

【００１０】また、一般にこのような通信を行うネットワークの構成は様々あり、例えば移動計算機とその通信相手とは直接接続されておらず、どのような通信経路を辿ってもホームルータを経由してしまう、といった場合もある。また、移動計算機と、その通信相手が同一のネットワーク内にいて、そのネットワークの外部へのゲー

5

トウェイで暗号化を行う通信を開始して、それらの２計算機のアドレスが判った場合、直接接続される経路がそれまで暗号化していたゲートウェイを通らなくなることもある。したがって、これらのような状況に対応可能な制御が必要になる。

【００１１】本発明は、上記事情を考慮してなされたものであり、複数の計算機が複数の相互接続された通信ネットワークにより互いに接続されて相互に通信可能に構成された計算機システムで、移動計算機の位置情報を管理する装置を介して暗号化通信が行われる際に、冗長な通信である可能性を検出して移動計算機とその通信相手双方に通知することで通信の冗長さを回避可能な通信経路制御方法および通信経路制御装置を提供することを目的とする。

【００１２】

【課題を解決するための手段】本発明（請求項１）は、通信網を介して他の計算機ネットワークに接続され、自組織ネットワーク内の所定の接続位置をホームとする計算機の現在位置を管理し転送されてきたパケットを宛先計算機に中継するホームルータ装置を備えた計算機ネットワークシステムにおいて、計算機間の通信経路を制御するための通信経路制御方法であって、前記計算機に固有の前記自組織ネットワーク内で一意に定められた第１の位置識別子と、該計算機のうちホームの接続位置から移動した計算機について該計算機が移動した位置を識別可能なネットワーク全体で一意に定められた第２の位置識別子とを対応付けたアドレス情報を記憶し、前記ホームルータ装置により中継されるパケット内に含まれる前記第１の位置識別子からなる送信元情報および宛先情報と前記アドレス情報とに基づいて、前記パケットを通信する２つの計算機夫々について、前記自組織ネットワーク内のホームの接続位置から移動しているものであるか否かを判断し、前記パケットを通信する２つの計算機のうち少なくとも一方が前記自組織ネットワーク内のホームの接続位置から移動しているものであると判断された場合、少なくとも該移動している計算機の通信相手に該移動している計算機に対する前記第２の位置識別子を送信することを特徴とする。

【００１３】また、上記判断の後、前記パケットを通信する２つの計算機が、いずれも前記自組織ネットワーク内のホームの接続位置から移動しているものであると判断された場合、前記２つの計算機に互いの通信相手の計算機に対する前記第２の位置識別子を送信するようにしても良い。

【００１４】好ましくは、前記第２の位置識別子とともに、該第２の位置識別子を用いて直接通信を確立すべき旨の制御情報を通信する。前記第２の位置識別子を受信した前記２つの計算機は、受信した前記第２の位置識別子を用いて前記ホームルータ装置を介さない直接通信の確立を試みる。

6

【００１５】本発明によれば、移動計算機とその通信相手の位置情報を検出し、該通信相手に該移動計算機の第２の位置識別子を通知し、ホームルータを経由することなく直接接続を行って通信する旨の制御情報を返信するので、従来ホームルータ装置を経由してのみ可能であった移動計算機とその通信相手とのデータ通信について、両者が直結可能であればそれ以降の通信効率を高くすることが可能である。これは、特に、両者がいずれも同じ組織に管理されるネットワーク内にあり、かつファイアウォールでガードされていて相互に暗号化通信が可能である場合に有効である。

【００１６】本発明（請求項２）は、請求項１において、前記第２の位置識別子を送信した後に、前記自組織ネットワーク内の前記ホームルータ装置を前記２つの計算機間にて通信されるパケットが再度通過したことが検出された場合、前記第２の位置識別子の送信先の計算機に前記自組織ネットワーク内の前記ホームルータ装置を経由した通信を行なう旨の制御情報を送信することを特徴とする。

【００１７】前記第２の位置識別子を受信した前記計算機が、受信した前記第２の位置識別子を用いて前記ホームルータ装置を介さない直接通信の確立を試みた結果、直接通信が確立できなかった場合、該当パケットは前記ホームルータ装置に送られて来るので、前記計算機に前記自組織ネットワーク内の前記ホームルータ装置を経由した通信を行なう旨の制御情報を送信することで、元の転送形態に戻す。

【００１８】本発明によれば、移動計算機とその通信相手とは直接接続されておらず、どのような通信経路を辿ってもホームルータを経由してしまう、といった場合、通知後、再度それらに計算機同士の通信データを受け取った場合は、元の転送形態に戻すようにするので、通信は何ら影響を受けず元の状態で再開できる。

【００１９】本発明（請求項３）は、請求項１において、前記判断にあたって、前記送信元情報に対応する前記第２の位置識別子と前記宛先情報に対応する前記第２の位置識別子とを比較して、前記２つの計算機夫々が同一のネットワーク内に存在するか否かを判定し、前記２つの計算機夫々が同一のネットワーク内に存在すると判定された場合、通信データに対するデータ加工処理（例えば、認証データなどのデータ付加処理や暗号化処理など）を行わず最短の経路で直接通信するよう通信経路を変更することを指示する制御情報をも送信することを特徴とする。

【００２０】本発明（請求項４）は、請求項３において、前記判定にあたって、前記２つの計算機間で通信される通信データに対するデータ加工処理の内容が変更されるか否かをも併せて判定し、直接通信を確立させると変更が生じる場合、前記第２の位置識別子及び前記制御情報を双方に返信しないことを特徴とする。

7

【００２１】本発明（請求項５）は、請求項３において、前記判断にあたって、前記２つの計算機間で通信される通信データに対するデータ加工処理の内容が変更されるか否かをも併せて判定し、直接通信を確立させると変更が生じる場合、前記制御情報に通信データのデータ加工処理の内容を変更させる指示情報を含めることを特徴とする。

【００２２】本発明によれば、移動計算機と、その通信相手が同一のネットワーク内にいて、そのネットワークの一部で暗号化を行う通信を開始した際、それらの２計算機を直結する経路がそれまで暗号化していた部分を通らない場合は、（ポリシー１）既に暗号化のための制御情報を相互に交換しているので、それをそのまま使用するため、経路を変更しない、（ポリシー２）同一組織であることが判明したので全く暗号化を行わない通信に切替える、（ポリシー３）直結経路で別の暗号化部分で暗号化通信できるなら、その暗号化部分を用いる暗号化通信を行うように切替える、といった３種類の柔軟な処理方法を適宜選択して処理を行うことができる。

【００２３】本発明（請求項６）は、通信網を介して他の計算機ネットワークに接続され、自組織ネットワーク内の所定の接続位置をホームとする計算機の現在位置を管理し転送されてきたパケットを宛先計算機に中継するホームルータ装置を備えた計算機ネットワークシステムにおいて、該自組織ネットワーク内の所定の接続位置をホームとする計算機間の通信経路を制御するための通信経路制御装置であって、前記計算機に固有の前記自組織ネットワーク内で一意に定められた第１の位置識別子と、該計算機のうちホームの接続位置から移動した計算機について該計算機が移動した位置を識別可能なネットワーク全体で一意に定められた第２の位置識別子とを対応付けたアドレス情報を記憶する手段と、前記ホームルータ装置により中継されるパケット内に含まれる前記第１の位置識別子からなる送信元情報および宛先情報と前記アドレス情報とに基づいて、前記パケットを通信する２つの計算機夫々について、前記自組織ネットワーク内のホームの接続位置から移動しているものであるか否かを判断する手段と、前記パケットを通信する２つの計算機のうち少なくとも一方が前記自組織ネットワーク内のホームの接続位置から移動しているものであると判断された場合、少なくとも該移動している計算機の通信相手に該移動している計算機に対する前記第２の位置識別子を送信する手段とを備えたことを特徴とする。

【００２４】好ましくは、前記第２の位置識別子とともに、該第２の位置識別子を用いて直接通信を確立すべき旨の制御情報を通信する。前記第２の位置識別子を受信した前記計算機は、受信した前記第２の位置識別子を用いて直接通信の確立を試みる。

【００２５】

【発明の実施の形態】以下、図面を参照しながら発明の実施の形態を説明する。図１に、本発明の一実施形態に係る計算機ネットワークシステムの基本構成を示す。図１のように、自組織ネットワーク１ａ、外部の自組織ネットワーク１ｂと１ｃが外部ネットワーク１ｄにより相互に接続されており、自組織ネットワーク１ａには、接続位置の固定されたホスト計算機や移動可能なホスト計算機が接続可能である。

【００２６】自組織ネットワーク１ａ，１ｂ，１ｃには、それらが管理する計算機間でデータ内容を（暗号化などにより）秘匿して通信を行うためのデータパケット処理装置４ａ，４ｂ，４ｃがそれぞれ設置されており、自組織の管理する計算機間の暗号化通信を達成する。なお、データパケット処理装置を持たない外部のネットワーク（図示せず）に移動した移動ホスト計算機内にデータパケット処理機能が搭載されている場合も同様に暗号化通信可能である。

【００２７】自組織ネットワーク１ａ内には、該自組織ネットワーク１ａ内の所定の接続位置をホームとする各ホスト計算機の位置情報を管理するホームルータＨＲが接続されている。

【００２８】図２は、ホスト計算機のアドレス管理のためにホームルータＨＲ内に設けるアドレス管理テーブルの一構成例を示す。アドレス管理テーブルは具体的には２つのアドレスを連結したテーブルとして実現される。ここで、ホームアドレスは移動ホスト計算機に固有の自組織のネットワーク内で一意に定められたアドレスを示し、移動先アドレスは移動ホスト計算機がネットワーク上で移動した現在位置を示すネットワーク全体で一意に定められたアドレスを示す。なお、移動先アドレスは、使用する移動通信プロトコルによっては、当該移動ホスト計算機の移動先ネットワーク内にて当該移動ホスト計算機をホームアドレスで管理する外部管理装置の位置を示すネットワーク全体で一意に定められたアドレスとなる。

【００２９】図１では自組織ネットワーク１ａをホームとする移動ホスト計算機Ｈ２とＨ３がそれぞれ外部の自組織ネットワーク１ｂと１ｃに移動中の場合を示しているが、これに対応して図２のアドレス管理テーブルには、ホスト計算機Ｈ２についてはホームアドレスＨＡ２と移動先アドレスＣＡ２が、ホスト計算機Ｈ３についてはホームアドレスＨＡ３と移動先アドレスＣＡ３が、それぞれ対応付けられて登録されている様子が示されている。また、ホスト計算機Ｈ１は、移動先アドレスを持たず、自組織ネットワーク１ａ内のホームの位置ＨＡ１に存在することが示されている。

【００３０】移動ホスト計算機の第２の識別子の登録は、例えば、移動ホスト計算機が移動先でネットワークに接続したときに、移動ホスト計算機からホームルータＨＲに第２の識別子を登録するための制御パケットを送信することでなされる。

【００３１】なお、このアドレス管理テーブルは、システム構成に応じて、バケット管理装置４上や他の図示しないサーバ計算機上など、ホームルータＨＲが参照可能な様々な場所に置くことが可能である。

【００３２】本実施形態では、自組織ネットワーク１ａをホームとする移動ホスト計算機間の通信経路を制御するための経路制御装置１２を備えている。この経路制御装置１２は、ホームルータＨＲ内に設けるものとしている。なお、経路制御装置１２は、ホームルータＨＲを経由するバケットを監視できればどのような位置に存在しても良く、例えば、データバケット処理装置４ａ内に設けても良いし、バス２０上に独立したノードとして接続しても良い。

【００３３】以下、自組織ネットワーク１ａをホームとする移動ホスト計算機間の通信と、経路制御装置１２の働きについて説明する。図３には経路制御装置１２の処理手順の流れを、図４には通信および制御の様子を示す。

【００３４】まず、本実施形態では、移動ホスト計算機Ｈ２とＨ３が、それぞれ外部の自組織ネットワーク１ｂと１ｃに移動中の場合を考える。ホスト計算機Ｈ２とその通信相手のホスト計算機Ｈ３とが相互に暗号化通信を行う場合、両ホスト計算機は、互いの現在位置が未確定であるので、ホームアドレスＨＡ２やＨＡ３で宛先を指定したデータバケットを、ホームルータＨＲに届くように（図４の場合にはホームルータＨＲについてネットワーク全体で一意に定められたアドレスＣＡ０を使用して）暗号化カプセル化し、両者が移動前に接続されていた自組織ネットワーク１ａのホームルータＨＲに向けて送り出す（図４の①）。

【００３５】ホスト計算機Ｈ２からのデータが到着すると、ホームルータＨＲは、暗号化されたデータを復号し、ヘッダ内に書かれたホームアドレスＨＡ３から、該バケットが移動中のホスト計算機Ｈ３宛てであることを知る。そして、ホームルータＨＲ内で管理されている図２のようなアドレス管理テーブルを参照し、移動ホスト計算機Ｈ３の現在位置情報を求める。この場合、移動先アドレスＣＡ３が現在の位置情報となるので、ホスト計算機Ｈ３の現在位置を示すネットワーク全体で一意なアドレスＣＡ３に転送先を変えて、ホスト計算機Ｈ３にデータバケットを送る（図４の②）。

【００３６】ホスト計算機Ｈ３からホスト計算機Ｈ２への通信も同様で、ホームルータＨＲ宛てに一度送られた（図４の③）データを復号し、ホスト計算機Ｈ２の現在位置情報に基づいて、ホスト計算機Ｈ２の現在位置を示すネットワーク全体で一意なアドレスＣＡ２に転送先を変えて、ホスト計算機Ｈ２にデータバケットを送る（図４の④）。

【００３７】ここで、ホームルータＨＲは、通信する２つの移動ホスト計算機Ｈ２，Ｈ３のネットワーク全体で一意であるアドレス情報を得られるので、そのアドレス情報を２つの移動ホスト計算機Ｈ２，Ｈ３に通知すれば、もし２つの移動ホスト計算機Ｈ２，Ｈ３間に直結するルートがある場合、ホームルータＨＲを通らない最適化された経路で通信させることが可能となる。

【００３８】そこで、本実施形態の経路制御装置１２は、次のような制御を行う。経路制御装置１２は、ホームルータＨＲを経由するデータバケット内の送信元アドレスと宛先アドレス（例えば上記したＨＡ２とＨＡ３）を元に、図２のようなアドレス管理テーブルを参照して、両計算機が移動中のものであるか調べる（ステップＳ１１）。

【００３９】例えば、該当移動計算機についてアドレス管理テーブルに移動先アドレスが登録されている場合は、移動中であると判断する。あるいは、アドレス管理テーブル内に設けた移動中フラグを参照する。

【００４０】そして、自身を中継点とする移動中計算機間の暗号化通信を検出すると（ステップＳ１２）、その通信を行う２つの移動ホスト計算機Ｈ２，Ｈ３に通信相手の現在位置を示すネットワーク全体で一意であるアドレスを通知し（ステップＳ１３）、両者に直結する最適化ルートで暗号化通信を再度セットアップする旨の制御コマンドを送付する。

【００４１】この例では、移動ホスト計算機Ｈ２に対しては通信相手である移動ホスト計算機Ｈ３の移動先アドレスＣＡ３を通知し、移動ホスト計算機Ｈ３に対しては通信相手である移動ホスト計算機Ｈ２の移動先アドレスＣＡ２を通知する（図４の⑤）。

【００４２】なお、上記のアドレスの送信のときに、暗号化通信を継続する旨の制御情報などを併せて送信しても良い。この制御コマンドを受けた移動ホスト計算機Ｈ２，Ｈ３により最適化経路による暗号化通信が達成されれば、以降その経路に沿って通信を行う（図４の⑥）。

【００４３】ところで、ネットワーク構成によっては、移動ホスト計算機Ｈ２と移動ホスト計算機Ｈ３の間をホームルータＨＲを通過せずに結ぶルートが存在しないこともある。そのような場合に対処するため、ホームルータＨＲが制御コマンドを送信した後で、直接通信が成立したか否かを監視する（ステップＳ１４）ことが望ましい。直接通信が成立しなかった場合には、再度２台のホスト計算機の通信をホームルータＨＲで受け取ることになるので、この監視により直接通信の成否を判断することができる。

【００４４】もし直接通信が成立しなかった場合（ステップＳ１５）、今までのサービスの継続、すなわちホームルータＨＲ経由の通信の提供のために必要な処理を行う（ステップＳ１６）。

【００４５】例えば、

（１）そのままホームルータＨＲ経由で直結通信させる（いままでの経路を有効として維持する）

あるいは、
（２）先に送った制御コマンドを無効とし、再度ホームルータＨＲ宛から双方のホスト計算機宛への２つの転送で通信させる
といった方法で対処できる。この２つの方法のいずれを選択するかは、要求される通信の速度、品質やネットワーク構成を考慮して決定すれば良い。

【００４６】このように本実施形態によれば、移動計算機とその通信相手の位置情報を検出し、両者にお互いの外部ネットワークアドレス（すべてのネットワーク上で一意に定まっている）を通知し、従来ホームルータを経由してのみ可能であった移動計算機とその通信相手とのデータ通信を、ホームルータを経由することなく直接接続を行う旨の制御情報を双方に返信するので、両者が直結可能であればそれ以降の通信効率を高くすることが可能である。これは、特に、両者がいずれも同じ組織に管理されるネットワーク内にあり、かつファイアウォールでガードされていて相互に暗号化通信が可能であると判断した場合に有効である。

【００４７】また、本発明によれば、移動計算機とその通信相手とは直接接続されておらず、どのような通信経路を辿ってもホームルータを経由してしまう、といった場合、通知後、再度それらに計算機同士の通信データを受け取った場合は、元の転送形態に戻すようにするので、通信は何ら影響を受けず元の状態で再開できる。

【００４８】次に、他の移動形態の通信例について図３を参照しながら説明する。この例は、移動ホスト計算機Ｈ２が移動した結果、その通信相手のホスト計算機３と同一のネットワークに入った場合である。この場合、まず、ネットワークの入口に置かれたデータパケット処理装置４ａでデータパケットが暗号化され（図５中の１０１）、その後、ネットワーク内のホームルータＨＲに転送され（１０２）、ホームルータＨＲが移動ホスト計算機Ｈ２の現在位置を識別し転送する（１０３）。データパケットは移動ホストＨ２に附属するデータパケット処理装置４ｄで復号化される。

【００４９】ここで、経路制御装置１２は、ホームルータＨＲ内にて管理されているホスト計算機Ｈ３と移動ホスト計算機Ｈ２の位置情報を参照することにより、両ホスト計算機が現在同じネットワーク内にあることを判断できる。２つの計算機が同一のネットワーク内に位置するか否かの判定は、例えば、計算機のネットワークアドレスの比較により実現できる。

【００５０】そこで、前記経路制御装置１２は、以下のような制御を行うと良い。すなわち、図６に示すように、ホームルータＨＲを経由するデータパケット内の送信元アドレスと宛先アドレスを解析し（ステップＳ２１）、もし両者が元々同一組織に属している計算機であり、外部ネットワークを通らずに通信できることがわかれば（ステップＳ２２）、暗号化／復号化が不要であると判断して、双方に互いの現在のアドレスを通知すると共に暗号化通信が不要である旨を通知する制御コマンドを発行し（ステップＳ２３）、暗号化せずかつ両者を直結する経路（図５中の１０４）でのより高速な通信を行わせる。

【００５１】ところで、２つのホスト計算機のうち少なくとも一方が外部から移動してそのネットワークに入ったものであり、同一ネットワーク上にあっても暗号化通信が必要である場合もありうる。このような場合、前述のように直ちに双方に互いの現在位置を示し、直結ルートで通信をセットアップすべき旨の制御コマンドを送り、別の直結ルートを使用させると、暗号化を行うデータパケット処理装置４ａ（ホームルータＨＲに附属している）を通過しなくなるための不具合が生じることがある。

【００５２】この不具合とは、
（１）もし直結ルート（図５中の１０４）に別のデータパケット処理装置（図５中の４ｅ）があれば、暗号化通信可能であるが、直結ルートに別のデータパケット処理装置がなければ、暗号化通信は行えない。
あるいは、
（２）直結ルート（図５中の１０４）に別のデータパケット処理装置（図５中の４ｅ）があっても、データパケット処理装置４ａからデータパケット処理装置４ｅに替えた場合、暗号化鍵の交換などを再度やり直さなければならない。
などの問題である。

【００５３】従ってこのような場合を想定して、経路制御装置１２は、以下のような制御を行うと良い。すなわち、図７のように、直接通信させて良いかを判断し（ステップＳ３３）、直接通信させると判断した場合にのみ（ステップＳ３４）、双方に互いの現在のアドレスを通知すると共に両者に直結する最適化ルートで暗号化通信を再度セットアップする旨の制御コマンドを発行し（ステップＳ３５）、両者を直結する経路でのより高速な通信を行わせる。

【００５４】上記の判断とは、例えば、
（１）もし直結ルートに別にデータパケット処理装置があれば、通信経路の変更を促す制御コマンドを双方に発行し、なければ経路変更はしない。
あるいは、
（２）経路変更によりデータパケット処理装置が変わることがありうる場合、経路変更はしない。これはネットワーク構成をホームルータＨＲにより検査してもよいし、双方に仮に直結ルートでの送受信を行わせ、暗号化を行うデータパケット処理装置の識別子をデータに付記したものをチェックしてもよい。
といった方法で処理を行う。いずれを選択するかは、要求される通信の速度、質やネットワーク構成を考慮して決定すれば良い。

13

【００５５】なお、通信データに対する認証処理などの内容が変更されるかどうかを判定する機構は、それら２つの計算機間の直結経路が、認証を行うルーター、ファイアウォールを経由するかの判定を行う機構として実現できる。

【００５６】本発明によれば、移動計算機と、その通信相手が同一のネットワーク内にいて、そのネットワークの一部で暗号化を行う通信を開始した際、それらの２つの計算機を直結する経路がそれまで暗号化していた部分を通らない場合は、（ポリシー１）既に暗号化のための制御情報を相互に交換しているので、それをそのまま使用するため、経路を変更しない、（ポリシー２）同一組織であることが判明したので全く暗号化を行わない通信に切替える、（ポリシー３）直結経路で別の暗号化部分で暗号化通信できるなら、その暗号化部分を用いる暗号化通信を行うように切替える、といった３種類の柔軟な処理方法を適宜選択して処理を行うことができる。

【００５７】次に、これまで説明してきた実施形態を変形した形態について説明する。以上の説明では、ホームルータＨＲ経由で通信する両方の計算機がともにホームの位置から移動中のものであった場合に、両者に互いの通信相手の現在位置を示すネットワーク全体で一意であるアドレスを通知することとした。その代わりに、一方の計算機がホームの位置から移動中のものであった場合にも、該移動中の計算機の通信相手に該移動中計算機の現在位置を示すネットワーク全体で一意であるアドレスを通知するようにしても良い。この場合、該通信相手から送り出される該移動中計算機宛のパケットを、ホームルータＨＲを経由せずに転送させることが可能になる。

【００５８】例えば、図１において、図示しない外部組織のネットワークに接続されている計算機Ｈｘと外部の自組織ネットワーク１ｂに移動中の計算機Ｈ２の通信について考えてみる。ここで、計算機Ｈｘの現在位置を示すネットワーク全体で一意であるアドレスをＣＡｘとする。

【００５９】通信初期においては、計算機Ｈｘは計算機Ｈ２のネットワーク全体で一意であるアドレス（すなわち移動先アドレスＣＡ２）を知らないので、計算機Ｈ２のホームアドレスＨＡ２で宛先を指定したデータパケットを、計算機Ｈ２が移動前に接続されていた自組織ネットワーク１ａのホームルータＨＲに届くように送り出す。そして、先に説明したのと同様に、ホームルータＨＲは、計算機Ｈｘからのパケットをホスト計算機Ｈ２に転送する。ここで、計算機Ｈｘはパケット内に書き込む送信元アドレスとして上記のＣＡｘを使用するものとする。

【００６０】一方、計算機Ｈ２は、計算機Ｈｘから転送されてきたパケットのヘッダ情報から、計算機Ｈｘのネットワーク全体で一意であるアドレス（すなわちＣＡｘ）を知ることができるので、計算機Ｈ２から計算機Ｈｘへのパケット転送は、ホームルータＨＲを介さずに行うことができる。

14

【００６１】ここで、経路制御装置１２は、ホームルータＨＲを経由するデータパケット内の送信元アドレスと宛先アドレス（例えば上記したＨＡ２とＣＡｘ）から、両計算機のうち一方の計算機Ｈ２がホームの位置から移動中のものであることが分かる。これは、アドレスＣＡｘに位置する計算機Ｈｘは、計算機Ｈ２の現在位置を示すネットワーク全体で一意であるアドレスを知らないということを意味する。そこで、計算機Ｈｘに、計算機Ｈ２の現在位置を示すネットワーク全体で一意であるアドレスＣＡ２を通知する。

【００６２】このようにすれば、計算機Ｈｘは、計算機Ｈ２宛のパケットの宛先アドレスとして、該計算機Ｈ２のネットワーク全体で一意であるアドレスＣＡ２を指定することができるようになるので、計算機Ｈｘから計算機Ｈ２への通信経路も、ホームルータＨＲを経由せず、冗長のないものにすることができる。

【００６３】なお、上記のような外部組織のネットワークに接続された計算機は、自組織ネットワークに対するセキュリティー上の観点から、自組織ネットワークをホームとする移動計算機の移動先アドレスを通知することが好ましくないものである場合がある。そこで、上記のように外部組織のネットワークに接続された計算機に自組織ネットワークをホームとする移動計算機の移動先アドレスを通知するにあたっては、例えば計算機Ｈｘが予め登録されたものであることが確認されたことを条件とするなど、所定のポリシーに従った条件を課すようにしても良い。

【００６４】本発明は、現在様々提案されている移動通信プロトコルに対して、本発明の構成要素を適宜組み合わせることで容易に実現が可能である。また、本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。特に、本発明は、様々な移動通信プロトコルに対して上述した実施の形態を適宜修正することで容易に実現が可能である。

【００６５】

【発明の効果】本発明によれば、移動計算機とその通信相手の位置情報を検出し、該通信相手に該移動計算機の位置を識別可能なネットワーク全体で一意に定められた位置識別子を通知し、従来ホームルータ装置を経由してのみ可能であった移動計算機とその通信相手とのデータ通信について、ホームルータ装置を経由することなく直接接続を行わせるよう制御するので、両者が直結可能であればそれ以降の通信効率を高くすることが可能である。

【図面の簡単な説明】

【図１】本発明の実施の形態に係るネットワーク構成を示す基本構成図

15　　16

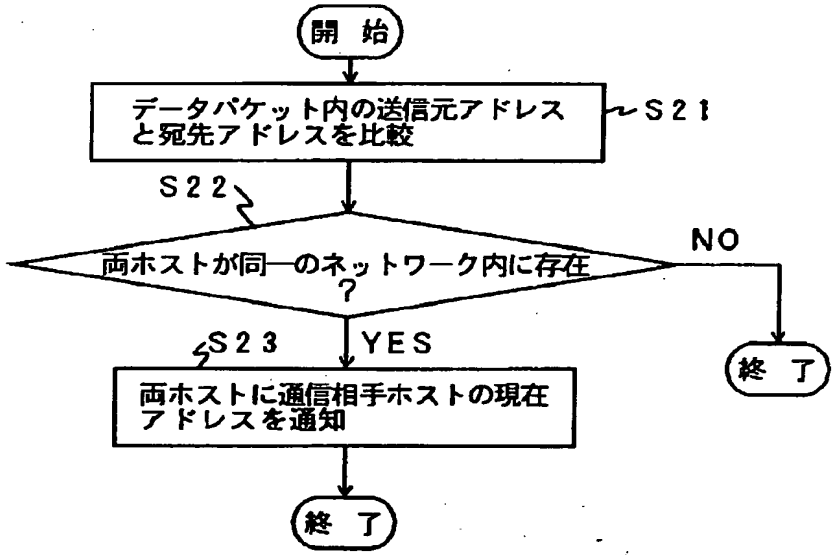
【図２】アドレス管理テーブルの一例を示す図
【図３】経路制御装置による制御の一例を示すフローチャート
【図４】本発明の実施の形態に係る経路最適化の制御コマンドの流れを示す図
【図５】本発明の実施の形態に係る他のネットワーク構成を示す基本構成図
【図６】経路制御装置による制御の一例を示すフローチャート
【図７】経路制御装置による制御の一例を示すフローチ＊10　＊ャート

【符号の説明】
１ａ…自組織ネットワーク
１ｂ，１ｃ…外部の自組織ネットワーク
１ｄ…外部ネットワーク
４ａ～４ｅ…データパケット処理装置
ＨＲ…ホームルータ
Ｈ１～Ｈ３…ホスト計算機
１２…経路制御装置
２０…バス

【図２】

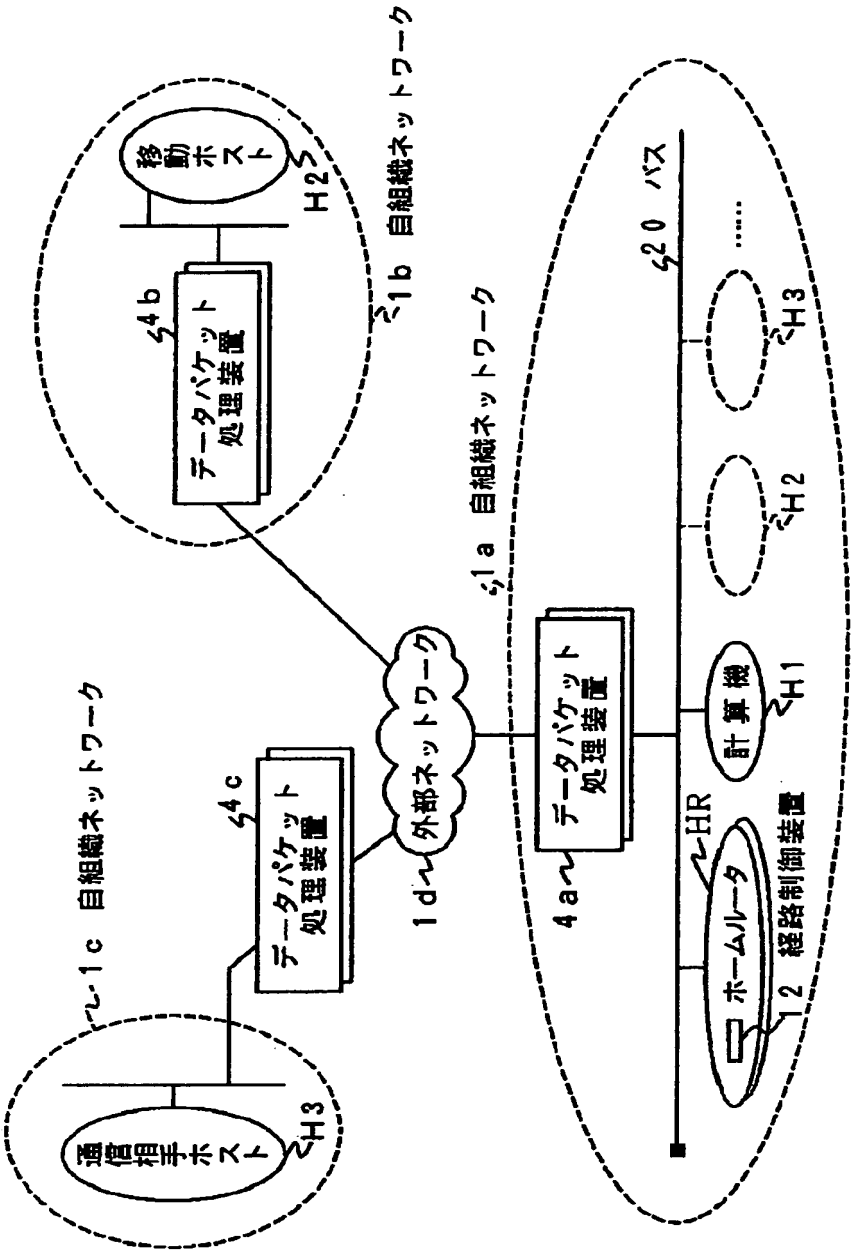
ホームアドレス	移動先アドレス
HA1	—
HA2	CA2
HA3	CA3
HA4	—
⋮	⋮

【図６】

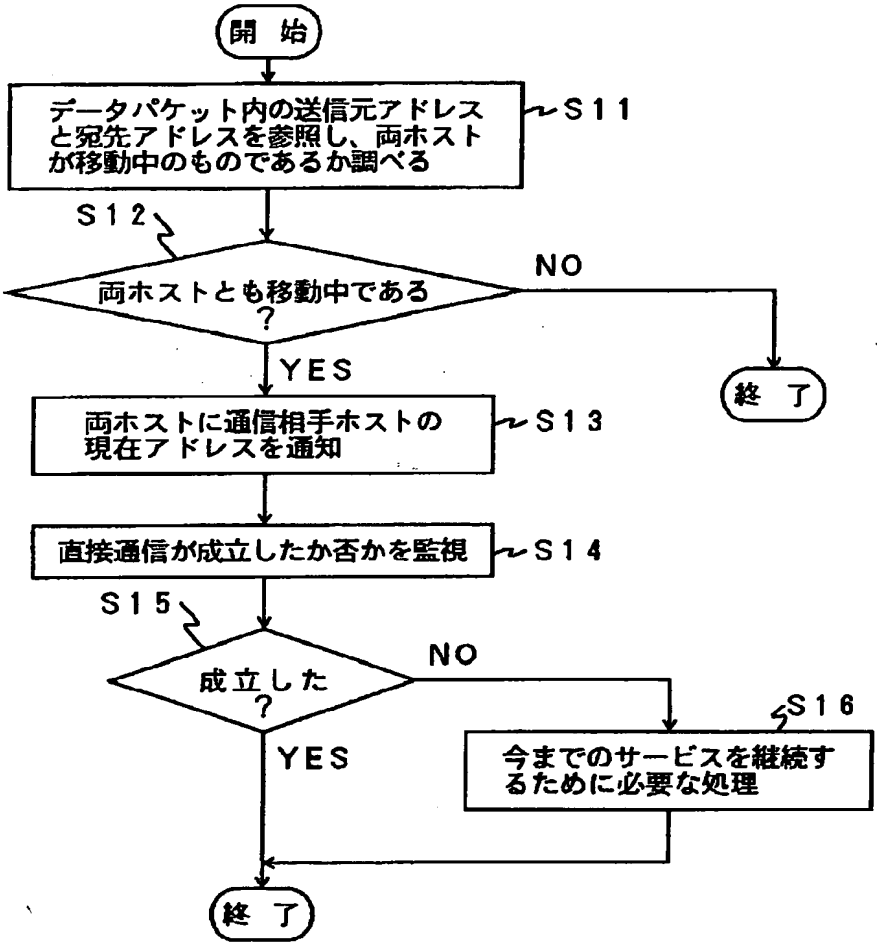


009.gif

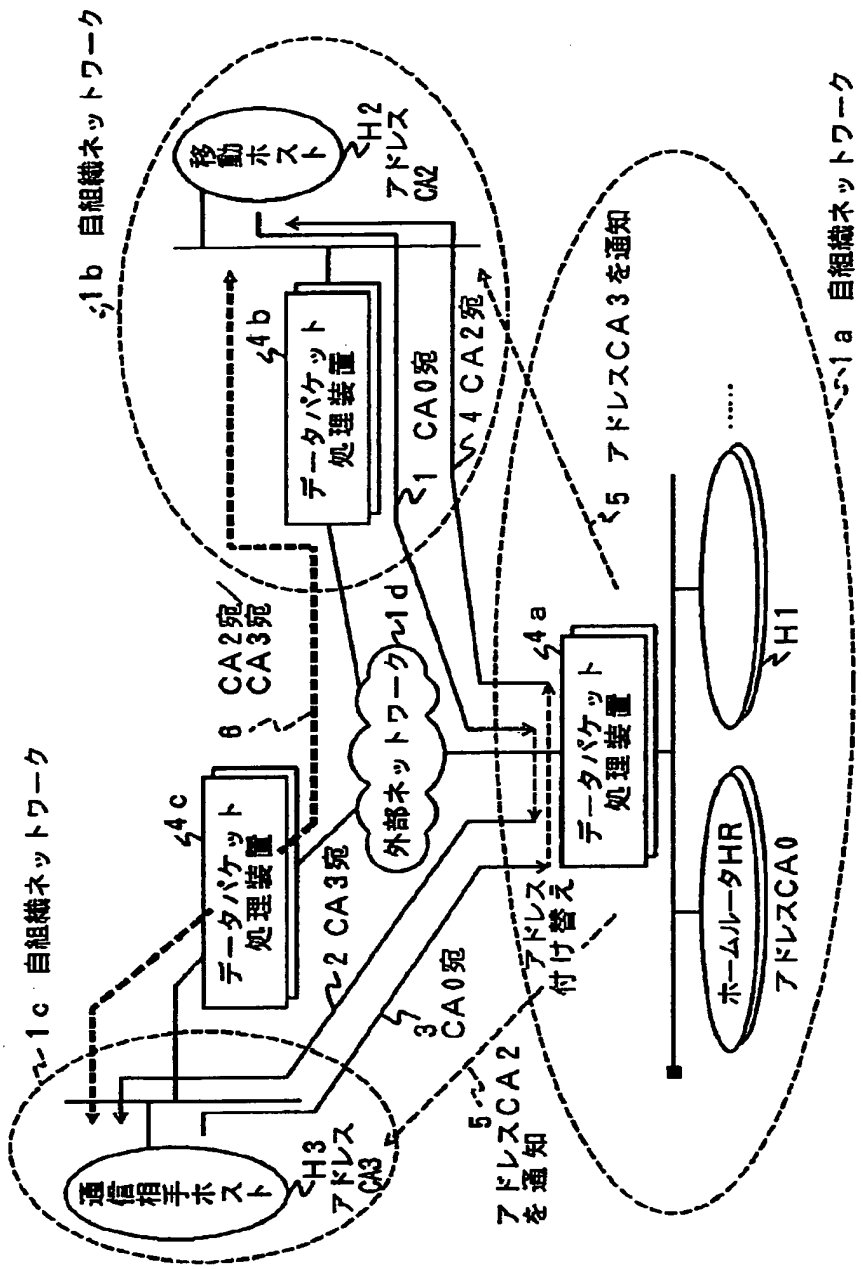
【図１】


1b 自組織ネットワーク
移動ホスト
H2
4b
データパケット処理装置
1a 自組織ネットワーク
20 バス
H3
H2
1c 自組織ネットワーク
4c
データパケット処理装置
1d
外部ネットワーク
4a
データパケット処理装置
計算機
H1
HR
ホームルータ
12 経路制御装置
通信端末ホスト
H3

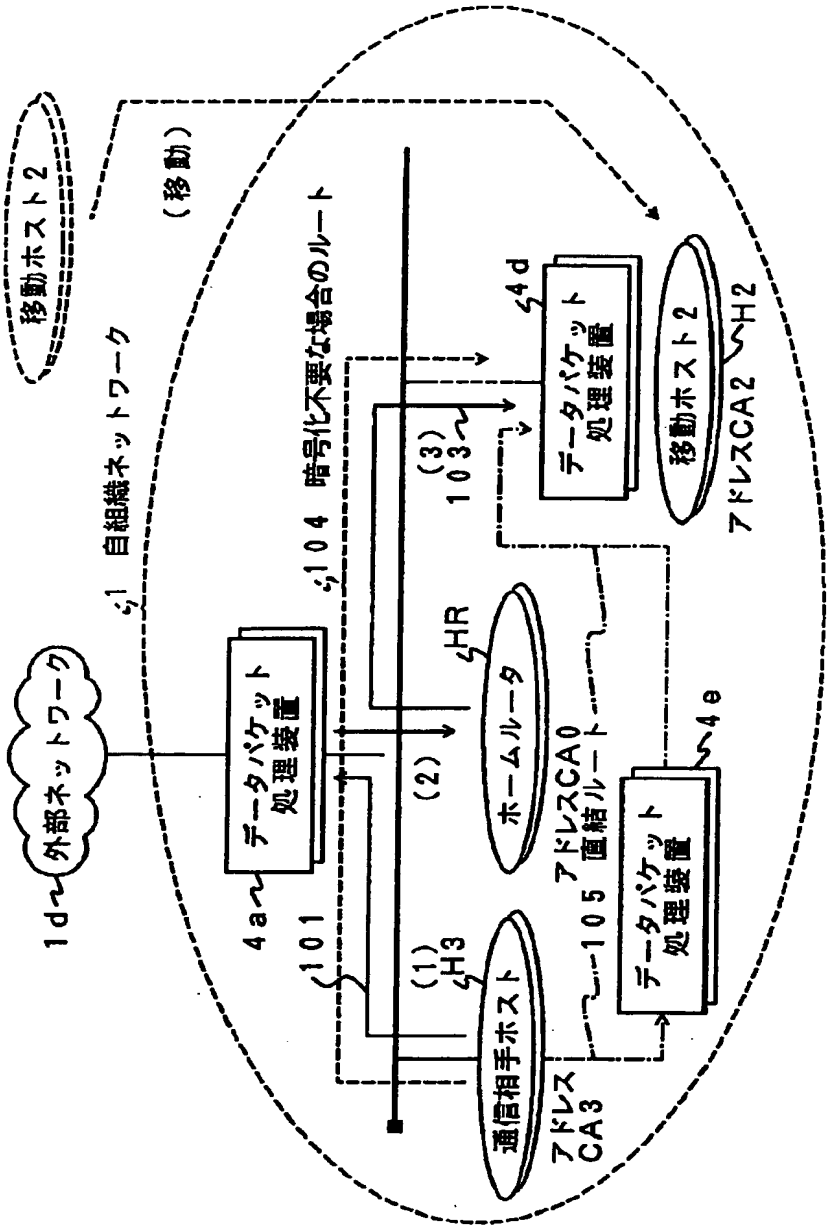
【図３】


開 始
データパケット内の送信元アドレスと宛先アドレスを参照し、両ホストが移動中のものであるか調べる
S11
S12
両ホストとも移動中である？
NO
YES
終 了
両ホストに通信相手ホストの現在アドレスを通知
S13
直接通信が成立したか否かを監視
S14
S15
成立した？
NO
YES
S16
今までのサービスを継続するために必要な処理
終 了

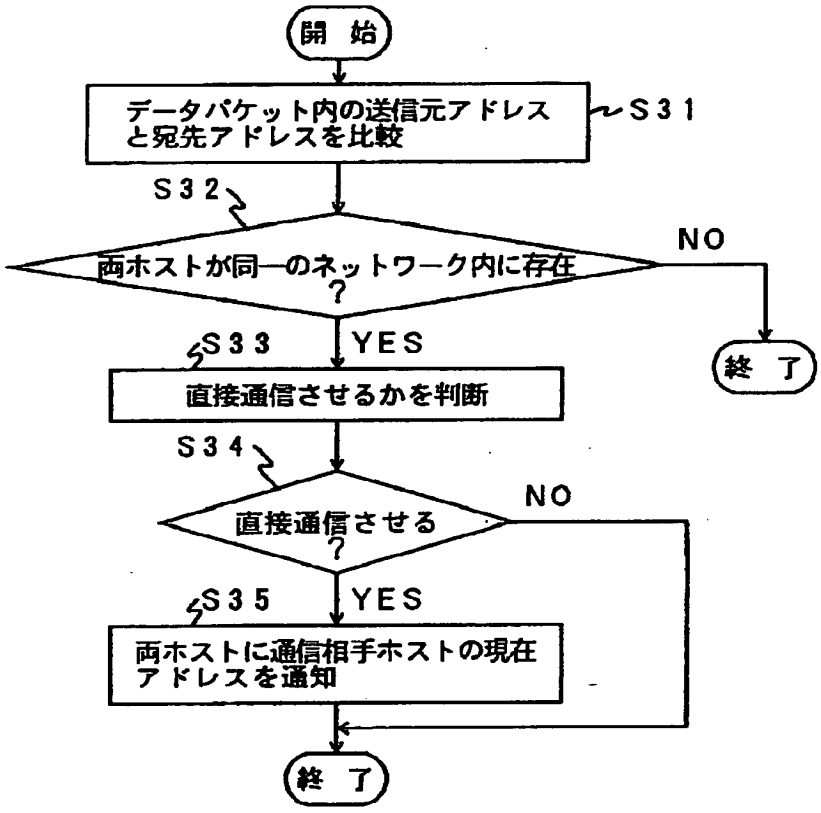
【図４】


1b 自組織ネットワーク
移動ホスト
H2
アドレス
CA2
データパケット
処理装置
4b
1 CA0宛
4 CA2宛
6 CA2宛
CA3宛
1d
外部ネットワーク
4c
データパケット
処理装置
2 CA3宛
3
CA0宛
1c 自組織ネットワーク
通信相手ホスト
H3
アドレス
CA3
5
アドレスCA2
を通知
アドレス
付け替え
4a
データパケット
処理装置
5 アドレスCA3を通知
1a 自組織ネットワーク
H1
ホームルータHR
アドレスCA0

【図5】


移動ホスト2
（移動）
1d
外部ネットワーク
1 自組織ネットワーク
104 暗号化不要な場合のルート
4a
データパケット処理装置
101
(1)
H3
通信相手ホスト
アドレスCA3
(2)
HR
ホームルータ
アドレスCA0
105 直結ルート
4e
データパケット処理装置
(3)
103
4d
データパケット処理装置
移動ホスト2
H2
アドレスCA2

【図７】



フロントページの続き

(72)発明者　新保　淳
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

(72)発明者　岡本　利夫
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内